

AMENDMENTS TO THE CLAIMS

1. (Canceled).

2. (Previously Presented) The method of claim 3 further wherein transferring comprises transferring a number of bytes specified by an operand from a memory.

3. (Currently Amended) A method comprising
configuring a cache memory of a processor to operate in a mode in which cache lines are not replaced;
transferring an ~~authenticated~~ a code module to the cache memory of the processor,
authenticating the ~~authentic~~ code module ~~storing~~ stored in the cache memory, ~~and~~
executing the ~~authenticated~~ code module from the cache memory in response to determining that the ~~authenticated~~ code module stored in the cache memory is authentic;
and
reconfiguring the cache memory to operate in a mode in which cache lines are replaced in response to cache misses.

4. (Currently Amended) The method of claim 3 further comprising invalidating the cache memory prior to storing the ~~authenticated~~ code module in the cache memory.

5. (Canceled).

6. (Currently Amended) The method of claim 3 further comprising determining whether the authenticated code module is authentic based upon a digital signature of the authenticated code module.

7. (Currently Amended) The method of claim 3 further comprising obtaining a first value from the ~~authenticated~~ code module stored in the cache memory;
computing a second value from the ~~authenticated~~ code module; and
determining that the ~~authenticated~~ code module is authentic in response to the first value and the second value having a predetermined relationship.

8. (Currently Amended) The method of claim 3 further comprising retrieving a key,
decrypting a digital signature of the ~~authenticated~~ code module with the key to obtain a first value,
hashing the ~~authenticated~~ code module to obtain a second value; and
executing the ~~authenticated~~ code module in response to the first value and the second value having a predetermined relationship.

9. (Currently Amended) The method of claim 8 wherein
decrypting comprises using the key to RSA-decrypt the digital signature, and
hashing comprises apply a SHA-1 hash to the ~~authenticated~~ code module to obtain the second value.

10. (Original) The method of claim 8 further comprising retrieving the key from the processor.

11. (Original) The method of claim 8 further comprising retrieving the key from a chipset.

12. (Previously Presented) The method of claim 8 further comprising retrieving the key from a token.

13. (Currently Amended) The method of claim 3 wherein transferring comprises receiving the ~~authenticated~~ code module from a machine readable medium.

14. (Canceled).

15. (Currently Amended) A computing device, comprising
a memory;
a memory controller coupled to the memory;
a machine readable medium interface to receive an ~~authenticated~~ a code module from a machine readable medium;
a private memory;
a separate private memory controller coupled to the private memory; and
a processor to transfer the authenticated code module from the machine readable medium interface to the private memory and to authenticate the authenticated code module stored in the private memory.

16. (Currently Amended) The computing device of claim 15, further comprising a key, wherein the processor authenticates the ~~authenticated~~ code module stored in the private memory based upon the key.

17. (Currently Amended) The computing device of claim 15, wherein the processor comprises a key and authenticates the ~~authenticated~~ code module stored in the private memory based upon the key of the processor.

18. (Currently Amended) The computing device of claim 14, further comprising a token, the token comprising a key, wherein the processor authenticates the ~~authenticated~~ code module stored in the private memory based upon the key of the token.

19-34. (Canceled).